Claims:

1. A method for performing a finite field multiplication of a first Galois element a, having bit places a_0 to a_{n-1}, provided to a first input register and a second Galois element b, having bit places b_0 to b_{n-1}, provided to a second input register, the Galois elements a and b belonging to a Galois field GF 2^n described by an irreducible polynomial PR with bit places PR_0 to PR_{n-1}, comprising forming in an addition part of a Galois multiplier an intermediate result Z of intermediate sums of partial products of bit width 2n - 2, said intermediate sums not representing any element of said Galois field, and processing said intermediate result Z in a reduction part of said Galois multiplier by modulo dividing by the irreducible polynomial PR, whereby after all XOR connections are traversed a result E, with bit places E_{n-1} to E_0 is computed.

2. A method according to claim 1, wherein said modulo dividing is carried out in two steps, in a first process stage all bit places Z_{2n-2} to Z_n are each AND connected with an expanded form PE of the irreducible polynomial PR having bit places PE_{n-1} to PE_0 and then assembled by a first parallel operating adder tree structure effectively realizing the operation XOR, and these assembled partial results are subsequently each AND connected in a second process stage with the bit places PR_{n-1} to PR_0 of the irreducible polynomial PR and using a second parallel-operating adder tree structure effecting the logic operation XOR, assembled with the bit places Z_{n-1} to Z_0 of the intermediate result Z to form the result E with bit places E_{n-1} to E_0.

3. A method according to claim 2, wherein a matrix PEM of bit place arrangement:

$$PEM = : \begin{matrix} (PE_{n-1,n-2...}PE_{n-1,0}) \\ (PE_{0,n-2...}PE_{0,0}) \end{matrix}$$

is precalculated with respect to an expanded form PE of said irreducible polynomial PR, and wherein said modulo dividing of said intermediate result Z is performed by AND connecting bits Z_{2n-2} to Z_n with the bit places of said matrix PEM and then, using a third parallel adder tree structure applying the multiple logic operation XOR, each assembled with the bit places Z_{n-1} to Z_0 of the intermediate result Z to yield the result E.

4. A method according to claim 2, wherein said first and second elements have respective variable bit widths va<a and vb<b with a resulting intermediate result Z having a bit width 2m - 2, wherein the bit places of the intermediate result Z are shifted $Z_{2mmax-2}$ - Z_m places in a decoder and field size adaptation logic prior to being connected with said expanded form PE of the irreducible polynomial PR, where the bit width 2mmax represents the maximum bit width of the intermediate result Z corresponding to each maximum bit width of the Galois elements a and b.

5. A method according to claim 3, wherein said first and second elements have respective variable bit widths va<a and vb<b with a resulting intermediate result Z having a bit width 2m - 2, wherein the bit places of the intermediate result Z are shifted $Z_{2mmax-2}$ - Z_m places in a decoder and field size adaptation logic prior to being AND connected with said matrix PEM of the irreducible polynomial PR, where the bit width

2mmax represents the maximum bit width of the intermediate result Z corresponding to each maximum bit width of the Galois elements a and b.

6. A finite field multiplier comprising a composite of individual cellular array multipliers assembled in a modulo reduction arrangement forming a most significant bit first matrix Galois multiplier, said Galois multipliers comprising an adder part, connected to first and second input registers, and including a partial product adder expansion structure and a partial product adder key structure connected together by first, second, third and fourth partial product expansion terminals; and a reducer part connected to receive an intermediate result output of said partial product adder and data derived from an irreducible polynomial PR, said reducer part arranged to combine said data and said intermediate result and provide a multiplication result to an output register.

7. A finite field multiplier as specified in claim 6, wherein the partial product adder key configuration comprises a first input of a first XOR adder element connected to a first partial product adder expansion terminal, wherein the first XOR adder element is connected with a second input to an output of a first XOR bit multiplier, wherein an output of the first XOR adder element is connected to a first intermediate result terminal, wherein said first XOR bit multiplier is connected with a first input to a bit place terminal a_{n-1}, wherein a second input of the first XOR bit place multiplier is connected to a bit place terminal b_{n-1}, wherein a first input of a second XOR adder element is connected to a second partial product expansion adder expansion terminal, wherein a second input of the second XOR adder element is connected to an output of a third XOR adder element,

wherein an output of the second XOR adder element is connected to a second intermediate result terminal, wherein a first input of the third XOR adder element is connected to an output of a second XOR bit multiplier element, wherein a second input of the third XOR adder element is connected to an output of a third XOR bit multiplier element, wherein a first input of the second XOR bit multiplier element is adjoined to the bit place terminal a_{n-1}, wherein a second input of the second XOR bit multiplier element is connected to a bit place terminal b_{n-2}, wherein a first input of the third XOR bit multiplier element is connected to a bit place terminal a_{n-2}, wherein a second input of the third XOR bit multiplier element is connected to a bit place terminal b_{n-1}, wherein an output of a fourth XOR adder element is connected to a first input of a fifth XOR adder element, wherein an output of the fifth XOR adder element is connected to a third intermediate result terminal, wherein an input of the fourth XOR adder element is connected to an output of a fourth XOR bit multiplier element, wherein a first input of the fourth XOR bit multiplier element is connected to the bit place terminal a_{n-1}, wherein a second input of the fourth XOR bit multiplier element is connected to said bit place terminal b_{n-2}, wherein a second input of the fourth XOR adder element is connected to an output of a fifth XOR bit multiplier element, wherein a first input of a fifth XOR bit multiplier element is connected to a said bit place terminal a_{n-2}, wherein a first input of the fifth XOR bit multiplier element is connected to said bit place terminal a_{n-2}, wherein a second input of the fifth XOR bit place multiplier element is connected to said bit place terminal b_{n-1}, wherein a second input of the fifth XOR adder element is connected to a fourth partial product adder expansion terminal, wherein an output of a sixth XOR adder element is connected to a fourth

intermediate result terminal, wherein a first input of the sixth XOR adder element is connected to an output of a sixth XOR bit multiplier element, the first input of which is connected in turn to said bit place terminal a_{n-2}, wherein a second input of the sixth XOR bit multiplier element is connected to said bit place terminal b_{n-2}, wherein a second input of the sixth XOR adder element is connected to a third partial product adder expansion terminal.

8. A finite field multiplier according to claim 6, wherein the reduction part consists of a modulo reduction apparatus containing a modulo reducer expansion structure and a modulo reducer key configuration.

9. A finite field multiplier according to claim 8, wherein said modulo reducer key configuration includes a first input of a first AND gate connected firstly to a first reducer intermediate result terminal and secondly to a second reducer expansion terminal, wherein a second input of said first AND gate is connected firstly to a first irreducible polynomial register terminal and secondly to a first input of a third AND gate, wherein an output of the first AND gate is connected to a first input of a first XOR connector, wherein a second input of the first XOR connector is connected to a second reducer intermediate result terminal, wherein an output of the first XOR connector is connected firstly to a first input of a third AND gate and further to a first reducer expansion terminal and moreover to a first input of a fourth AND gate, wherein an output of the third AND gate is connected to a first input of a third XOR connector, wherein an output of a third XOR connector is connected to a result register terminal E_{n-1}, wherein a second input of a

second AND gate is connected firstly to a second irreducible polynomial register terminal and moreover to a second input of the fourth AND gate, wherein an output of the fourth AND gate is connected to a first input of a fourth XOR connector, wherein an output of the fourth XOR connector is connected to a result terminal E_{n-2}, wherein an output of the second AND gate is connected to a first input of a second XOR connector, wherein a second input of the second XOR connector is connected to a reducer intermediate result terminal, wherein an output of the second XOR connector is connected to a second input of the third XOR connector and wherein a second input of the fourth XOR connector is connected to a fourth reducer intermediate result terminal.

10. A finite field multiplier according to claim 6, wherein said reduction part consists of a reduction two-step adder apparatus containing a two-step adder expansion structure and a two-step adder key configuration.

11. A finite field multiplier according to claim 10, wherein said two-step adder key configuration comprises a fifth cell gate having a first impart connected firstly to a first input of a seventh cell gate and moreover to the first intermediate result terminal, wherein a second input of the fifth cell gate is connected firstly to a second preset register terminal and secondly to a first input of an eighth cell gate, wherein a second input of the eighth cell gate is connected to the second intermediate result terminal, wherein an output of the eighth cell gate is connected to a first input of a first expansion adder, wherein an output of the seventh cell gate is connected to a second input of the first expansion adder, wherein a second input of the seventh cell gate is connected to a first preset register

terminal, wherein an input of the fifth cell gate is connected to a first input of a first expansion adder, wherein a second input of the first expansion adder is connected to a sixth reduction expansion terminal, wherein an output of the first expansion adder is connected firstly to a first input of a sixth cell gate and secondly to a ninth reduction expansion terminal, wherein a second input of the sixth cell gate is connected firstly to the second irreducible polynomial register terminal and secondly to a first input of a tenth cell gate, wherein an output of the first expansion adder is connected to a first input of a second expansion adder, wherein a second input of the second expansion adder is connected to a fifth reducer expansion terminal, wherein a first input of a ninth cell gate is connected to the first irreducible polynomial register terminal, wherein a second input of the ninth cell gate is connected firstly to an input of the second expansion adder and secondly to a second input of the tenth cell gate and moreover to a tenth reduction expansion terminal, wherein an output of the ninth cell gate is connected to a first input of a second output adder, wherein an output of the sixth cell gate is connected to a second input of the second output adder, wherein an output of the second output adder is connected to a first input of a third output adder, wherein a first input of a first output adder is connected to a seventh reduction expansion adder, wherein a second input of the first output adder is connected to the third intermediate result terminal, wherein an output of the first output adder is connected to a second input of the third output adder, wherein an output of the third output adder is connected to the result terminal E_{n-1}, wherein an output of the tenth cell gate is connected to a first input of a fourth output adder, wherein a second input of the fourth output adder is connected to the fourth intermediate result

terminal, wherein an output of the fourth output adder is connected to a first input of a fifth output adder, wherein a second input of the fifth output adder is connected to an eighth reduction expansion terminal, wherein an output of the fifth output adder is connected to the result terminal E_{n-2}.

12. A finite field multiplier according to claim 5, wherein the reduction part consists of a reduction one-step adder apparatus containing a one-step adder expansion structure and a one-step key configuration.

13. A finite field multiplier according to claim 11, wherein said one-step adder key configuration includes a first input of a second cell gate is connected firstly to the first intermediate result terminal and secondly to a first input of a first cell gate, wherein a second input of the second cell gate is connected to a first PEM terminal, wherein an output of the second cell gate is connected to a first input of a first XOR partial adder, wherein a second input of the first XOR partial adder is connected to a third reducer expansion terminal, wherein a second input of the first cell gate is connected to a fourth PEM terminal, wherein a first input of a fourth cell gate is connected firstly to the second intermediate result terminal and secondly to a first input of a third cell gate, wherein a second input of the fourth cell gate is connected to a second PEM terminal, wherein an output of the fourth cell gate is connected to a first input of a second XOR partial adder, wherein a second input of the second XOR partial adder is connected to the third intermediate result terminal, wherein an output of the second XOR partial adder is connected to a first input of a third XOR partial adder, wherein an output of the first XOR

partial adder is connected to a second input of the third XOR partial adder, wherein an output of the third XOR partial adder is connected to the result terminal E_{n-1}, wherein an output of the third cell gate is connected to an input of a fifth XOR partial adder, wherein a second input of the third cell gate is connected to a third PEM terminal, wherein an output of the first cell gate is connected to a first input of a fourth XOR partial adder, wherein a second input of the fourth XOR partial adder is connected to a fourth reducer expansion terminal, wherein a second input of the fifth XOR partial adder is connected to the fourth intermediate result terminal, wherein an output of the fifth XOR partial adder is connected to a first input of a sixth XOR partial adder, wherein an output of the fourth XOR partial adder is connected to a second input of the sixth XOR partial adder, and wherein its output is connected to the result terminal E_{n-2}.

14. A finite field multiplier according to claim 6, including a Galois multiplier accumulator, including said Galois multiplier, said first input register, said second input register, at least one of said expanded form and said irreducible polynomial PR, said result register and an adder, the output of the Galois multiplier being connected to the input of said adder and an output of said adder to the input of the result register, and the output of the result register being connected to one of the first input register and the second input register.

15. A finite field multiplier according to claim 6, including a Galois multiplier accumulator including said Galois multiplier, said first input register, said second input register, a preset register bank containing a matrix PEM, said result register and an adder,

the output of the Galois multiplier being connected to the input of the adder, and an output of the adder being connected to an input of the result register and an output of the result register being connected to an input of one of the first input register and the second input register.

16. A digital signal processor having a multiplier arranged to carry out the method of claim 1.

17. A digital signal processor having a multiplier arranged to carry out the method of claim 2.

18. A digital signal processor having a multiplier arranged to carry out the method of claim 3.

19. A digital signal processor having a multiplier arranged to carry out the method of claim 4.

20. A digital signal processor having a multiplier arranged to carry out the method of claim 5.

21. A digital signal processor having a finite field multiplier as specified in claim 6.

22. A digital signal processor having a finite field multiplier as specified in claim 7.

23. A digital signal processor having a finite field multiplier as specified in claim 9.

24. A digital signal processor having a finite field multiplier as specified in claim 11.

25. A digital signal processor having a finite field multiplier as specified in claim 13.

26. A digital signal processor having a finite field multiplier as specified in claim 14.

27. A digital signal processor having a finite field multiplier as specified in claim 15.